CLAIMS:

1. A mobile system, comprising:

a host chipset;

a locator subsystem connected to the host chipset and arranged to determine a current location of the mobile system; and

a main storage connected to the host chipset and arranged to store an operating system (OS) and contain an OS-Present application and/or a Pre-OS application configured to enforce security policies during user authentication, to access the locator subsystem and determine whether the mobile system may have been stolen or used inappropriately based on the security policies.

2. The mobile system as claimed in claim 1, wherein said main storage comprises:

a main memory arranged to store the operating system (OS), and the OS-Present application which is executed while the operating system (OS) is present; and

a flash memory arranged to store the Pre-OS application which is executed during boot up before the operating system (OS) is loaded.

3. The mobile system as claimed in claim 2, further comprising:

a protected storage configured to support the Pre-OS application and the OS-Present

application and to store configuration data, the security policies, authentication data and other information obtained from the Pre-OS application and the OS-Present application.

4. The mobile system as claimed in claim 3, further comprising:

a first interface arranged to provide the Pre-OS application access to the protected storage; and

a second interface arranged to provide the OS-Present application access to the protected storage.

5. The mobile system as claimed in claim 3, wherein said protected storage is a non-volatile readable and writeable memory device.

6. The mobile system as claimed in claim 3, wherein said locator subsystem corresponds to a radio-frequency (RF) based locator subsystem for determining the current location of the mobile system.

7. The mobile system as claimed in claim 6, wherein said security policies for the Pre-OS application and the OS-Present application include a designated number of failed log-on attempts, an unauthorized change attempted on selected platform policies, an unauthorized use of monitored services, a designated time expiration based on a renewable certificate, or a lack of communication to a policy server or to a security token, and an unauthorized deletion of the

protected storage.

8. The mobile system as claimed in claim 7, wherein said Pre-OS application corresponds to a system basic input/output start-up (BIOS) that is configured in accordance with Intel® Protected Access Architecture (IPAA) described in Application Interface Specification, Revision 1.0, and that is executed during boot up before the operating system (OS) is loaded.

9. The mobile system as claimed in claim 8, wherein said system BIOS is executed during boot up to check a Pre-OS security policy record, collect location based information from the RF-based locator subsystem, determine if there is a violation of the security policies during user authentication and, if there is a violation of the security policies, make a decision that the mobile system may have been stolen or used inappropriately.

10. The mobile system as claimed in claim 9, wherein said system BIOS is executed during boot up to further report the location of the mobile system to a proper authority, via an Internet or a RF-based wireless network.

11. The mobile system as claimed in claim 7, wherein said OS-Present application is executed to obtain an OS security record, check location based information, determine if an action is required based on the security policies and, if an action is required, then report a violation to an OS readable location in the protected storage and/or an external event monitoring

facility.

12. The mobile system as claimed in claim 11, wherein said RF-based locator subsystem corresponds to a Global Positioning System (GPS) receiver connected to the host chipset and arranged to contain an antenna complex for receiving the current location of the mobile system.

13. The mobile system as claimed in claim 11, wherein said RF-based locator subsystem corresponds to a RF transmitter that is part of a stolen device recovery system to provide location based information and is activated upon an occurrence of a trigger event to broadcast a silent, coded radio signal to the stolen device recovery system, via a radio tower, for enabling the police to track and recover the stolen device.

14. The mobile system as claimed in claim 11, wherein said RF-based locator subsystem corresponds to a Bluetooth™ transceiver that is part of a Bluetooth™ based security system including a central security server and a network of Bluetooth (voice/data) Access Points (BTAPs) installed in a designated area to provide security services for the mobile system, including asset control, remote monitoring and tracking of the mobile system, through the Internet or the RF-based wireless network.

15. A mobile system comprising:

a host chipset;

a RF-based locator subsystem connected to the host chipset and arranged to determine a current location of the mobile system;

a main memory connected to the host chipset and arranged to store an operating system (OS) and an OS-Present application executed while the operating system (OS) is present; and

a flash memory connected to the host chipset and arranged to store a Pre-OS application executed during boot up before the operating system (OS) is loaded and configured to enforce security policies during user authentication, to access the RF-based locator subsystem and determine whether the mobile system may have been stolen or used inappropriately based on the security policies.

16. The mobile system as claimed in claim 15, wherein said security policies include a designated number of failed log-on attempts, an unauthorized change attempted on selected platform policies, an unauthorized use of monitored services, a designated time expiration based on a renewable certificate, or a lack of communication to a policy server or to a security token, and an unauthorized deletion of the protected storage.

17. The mobile system as claimed in claim 16, wherein said Pre-OS application corresponds to a system basic input/output start-up (BIOS) that is configured in accordance with Intel® Protected Access Architecture (IPAA) described in Application Interface Specification, Revision 1.0, and that is executed during boot up before the operating system (OS) is loaded.

18. The mobile system as claimed in claim 17, wherein said system BIOS is executed during boot up to check a Pre-OS security policy record, collect location based information from the RF-based locator subsystem, determine if there is a violation of the security policies during user authentication and, if there is a violation of the security policies, make a decision that the mobile system may have been stolen or used inappropriately.

19. The mobile system as claimed in claim 18, wherein said system BIOS is executed during boot up to further report the current location of the mobile system to a proper authority, via an Internet or a RF-based wireless network.

20. The mobile system as claimed in claim 15, wherein said OS-Present application is executed to obtain an OS security record, check location based information, determine if an action is required based on the security policies and, if an action is required, then report a violation to an OS readable location in the protected storage and/or an external event monitoring facility.

21. The mobile system as claimed in claim 15, wherein said RF-based locator subsystem corresponds to a Global Positioning System (GPS) receiver connected to the host chipset and arranged to contain an antenna complex for receiving the current location of the mobile system.

22. The mobile system as claimed in claim 15, wherein said RF-based locator subsystem corresponds to a RF transmitter that is part of a stolen device recovery system to provide location based information and is activated upon an occurrence of a trigger event to broadcast a silent, coded radio signal to the stolen device recovery system, via a radio tower, for enabling the police to track and recover the stolen device.

23. The mobile system as claimed in claim 15, wherein said RF-based locator subsystem corresponds to a Bluetooth™ transceiver that is part of a Bluetooth™ based security system including a central security server and a network of Bluetooth (voice/data) Access Points (BTAPs) installed in a designated area to provide security services for the mobile system, including asset control, remote monitoring and tracking of the mobile system, through the Internet or the RF-based wireless network.

24. A computer readable medium having stored thereon a set of system basic input/output start-up "system BIOS" instructions configured in accordance with Intel® Protected Access Architecture (IPAA) which, when executed by a processor during start-up, cause the processor to perform:

initializing and testing a system platform;

checking a Pre-OS security policy record for an approved trigger mechanism;

collecting location based information from the approved trigger mechanism;

determining if there is a violation of security policies during user authentication; and

if there is a violation of the security policies, making a decision that the mobile system may have been stolen or used inappropriately.

25. The computer readable medium as claimed in claim 24, wherein said system BIOS instructions further cause the processor to report the location based information indicating the current location of the mobile system to a proper authority, via an Internet or a RF-based wireless network, when there is a violation of the security policies.

26. The computer readable medium as claimed in claim 24, wherein said security policies for the system BIOS instructions include a designated number of failed log-on attempts, an unauthorized change attempted on selected platform policies, an unauthorized use of monitored services, a designated time expiration based on a renewable certificate, or lack of communication to a policy server or to a security token, and an unauthorized deletion of a protected storage.